

LEGAL GUIDELINES

All NYPD Twitter pages contain a disclaimer that Twitter is not a venue to report emergencies or quality of life complaints. However, if members of the public tweet either, we have a duty to address them when we see them. We do not however, have a duty to monitor Twitter 24/7.

Allegations of corruption or misconduct that are tweeted should be treated the same way as if they were called in, reported by a walk in, or sent via letter. Follow patrol guide sections 207-22 and 207-31.

IT GUIDELINES

Users can protect themselves by following simple best practices. DCIT has implemented these mandatory policies:

- Only NYPD approved devices can be used to access Twitter - Personal devices shall never be used unless approved.
- Strong passwords for Twitter accounts are required.
- **NEVER** give the account username and password to anyone, ever, for any reason.
- **ALWAYS** use Twitter's multi-factor authentication feature, requiring a login code sent by SMS message to the user's NYPD phone.

LEGAL GUIDELINES

Only Twitter can remove tweets. According to their policy they will only remove the following types of tweets:

- Threatening violence against others
- Revealing other people's private information without their consent (addresses, credit card numbers, etc.)
- Tweets advocating unlawful or illegal activities
- Pornography or obscenity

Tweets are first amendment protected speech.

LEGAL GUIDELINES

We have an obligation to remove stale information - wanted posters, missing persons, etc.

Do not post prisoner photographs taken while in custody.

If we post photos related to an arrest, such as evidence recovered, we should put the ADA handling the prosecution on notice of the posting.

IT GUIDELINES

Computer and Operating Systems (including mobile devices) must have the latest patches, approved permissions/account configuration, antivirus engine and antivirus signatures.

- NEVER click on URLs provided in DMs or @ communications. If a legitimate party needs to communicate a URL to the NYPD, ask them to send it over email (this has the double advantage of requiring an exchange that will prove the other party isn't a bot).

IT GUIDELINES

Accessing shortened URLs is prohibited. A URL expander ***must*** be employed to view the full URL before accessing it.

- Access to the NYPD Official Twitter accounts is authorized via HootSuite only. Other third party applications, or access via twitter.com are not authorized.
- Log out of HootSuite and close the browser when not in use. This means closing ***all*** tabs in the browser, and all instances of separate windows of that browser.

LEGAL GUIDELINES

All NYPD Twitter pages contain a disclaimer that Twitter is not a venue to report emergencies or quality of life complaints. However, if members of the public tweet either, we have a duty to address them when we see them. We do not however, have a duty to monitor Twitter 24/7.

Allegations of corruption or misconduct that are tweeted should be treated the same way as if they were called in, reported by a walk in, or sent via letter. Follow patrol guide sections 207-22 and 207-31.

LEGAL GUIDELINES

Only Twitter can remove tweets.

According to their policy they will only remove the following types of tweets:

- Threatening violence against others
- Revealing other people's private information without their consent (addresses, credit card numbers, etc.)
- Tweets advocating unlawful or illegal activities
- Pornography or obscenity

Tweets are first amendment protected speech.

LEGAL GUIDELINES

We have an obligation to remove stale information - wanted posters, missing persons, etc.

Do not post prisoner photographs taken while in custody.

If we post photos related to an arrest, such as evidence recovered, we should put the ADA handling the prosecution on notice of the posting.

IT GUIDELINES

Users can protect themselves by following simple best practices. DCIT has implemented these mandatory policies:

- Only NYPD approved devices can be used to access Twitter - Personal devices shall never be used unless approved.
- Strong passwords for Twitter accounts are required.
- **NEVER** give the account username and password to anyone, ever, for any reason.
- **ALWAYS** use Twitter's multi-factor authentication feature, requiring a login code sent by SMS message to the user's NYPD phone.

IT GUIDELINES

Computer and Operating Systems (including mobile devices) must have the latest patches, approved permissions/account configuration, antivirus engine and antivirus signatures.

- NEVER click on URLs provided in DMs or @ communications. If a legitimate party needs to communicate a URL to the NYPD, ask them to send it over email (this has the double advantage of requiring an exchange that will prove the other party isn't a bot).

IT GUIDELINES

Accessing shortened URLs is prohibited. A URL expander ***must*** be employed to view the full URL before accessing it.

- Access to the NYPD Official Twitter accounts is authorized via HootSuite only. Other third party applications, or access via twitter.com are not authorized.
- Log out of HootSuite and close the browser when not in use. This means closing ***all*** tabs in the browser, and all instances of separate windows of that browser.